DELIVERY OF GOODS FROM INTERNET VENDORS TO ANONYMOUS CUSTOMERS

Background of the Invention

Field of the Invention

This invention relates generally to the processing of transactions over a computer network such as the Internet and, more particular, to the delivery of digital goods or services to customers by Internet vendors without the vendor knowing the identity of the customer.

Description of the Related Art

It is now commonplace for consumers to purchase goods or services from on-line or e-commerce retailers. A large number of retailers have set up sites where consumers can peruse the products that are available for sale, purchase the good, or goods, in question and have the product delivered to them. Although these goods are often tangible goods, substantial traffic in digital goods, such as electronic books, music, or application software is increasing.

The electronic good may be delivered directly from the on-line merchant's computer system. However this requires the on-line merchant to maintain a copy of the digital goods that it wants to sell. If a single on-line merchant is selling the electronic products of a number of vendors of electronic content, then the merchant is typically required to inventory and manage a large amount of material for each vendor.

A second option is to redirect the customer, after his or her purchase, to a computer server maintained by the vendor. The customer can then follow the instructions at the web site of the vendor to download the product. The customer must identify himself or herself, or present some form of credential to download the purchased product. This additional step requires the customer to expose his or her identity to the vendor and to follow the particular details of the download process that that vendor utilizes. This becomes especially complicated when the customer has purchased goods that are provided by a multiplicity of vendors. The user interface and

experience at each site is likely to be different, increasing the likelihood of customer confusion and greatly diminishing the on-line shopping experience. Further, placing the onus on the customer to get the product from the vendor by themselves, increases the likelihood that in the future, they will look to the vendor, rather than the merchant, as the source of these types of products.

If an authentication or authorization credential is given to the customer to allow him or her to request delivery of the product, attempts to steal or intercept the credential prior to its use by the legitimate customer are possible. This approach also requires the vendor to have a mechanism to prevent the re-use of credentials and to manage the access and credential verification of customers.

More preferable would be a system whereby the customer, after the purchase, may gain access to products maintained by one or more vendors without inconveniencing the customer, forcing him or her to reveal his or her identity, or putting the security of the transaction at risk, while maintaining the continuity of the shopping experience.

Summary of the Invention

The invention provides a system and associated methods that allow a customer to purchase a digital product from an on-line merchant, and then receive the product over a computer network from a vendor of the product, without revealing the customer's identity or other personal information to the vendor. Further, in some embodiments, the invention allows the merchant to maintain a common user purchase experience for a plurality of vendors, further enhancing the ease of the on-line shopping experience for the customer.

In a preferred embodiment, when a customer purchases a digital product from the on-line merchant, the merchant, through its computer system, creates an order record and order receipt for the transaction, and conveys the order receipt to the customer's computer. The order receipt contains the information used by the customer to request delivery of the product or products. In one embodiment, the conveyance of the order receipt from the merchant to the customer is via an email message. The email message contains a Uniform Resource Locator (URL) tag that allows the customer to bring up a

web page containing a list of the products ordered and, optionally, other information, such as order status information. The customer then selects the product to be delivered and the merchant issues a series of electronic requests to the vendor to initiate delivery of the product to the customer. After completion of delivery of the product to the customer, the vendor, through it's order processing system, notifies the merchant of the fulfillment of the delivery request and the merchant updates the order record to indicate that the product has been delivered.

In some embodiments of the invention, specific steps are taken to ensure that the entire receipt delivery, delivery request, and delivery processes are robust, secure, and present a simple and uniform shopping experience for the customer. The URL in the order receipt contains information that identifies the order. This information is strongly encrypted and encoded prior to its transport to the customer. This allows the merchant to trust the validity of a request when it is received, and inhibits or prevents third parties from obtaining delivery of items that others ordered.

In a preferred embodiment, when the customer uses the URL to access order information, the customer is presented with a list of the products that have been purchased but not yet downloaded. The customer may then select one of these products for delivery. The merchant then creates a secure hash made up of the relevant product and order information, such as the order ID, the item ID, the instance ID, the date, the time, etc. The merchant then sends this hash to the vendor. In some embodiments, this secure hash may be included in the original URL sent to the customer; and therefore does not need to be generated upon access by the customer. This also allows for the customer to directly access the vendor's order server, rather than going through the merchant.

Upon receipt of the request containing the hash, either from the customer or the merchant, the vendor de-hashes the secure hash to recover the order information inside it. Some types of products or configuration of vender order processors may require the merchant to send multiple communications to the vendor. This is often the case when the vendor's order processor has been designed assuming that the access will come from an interactive user. In these cases, the merchant emulates the actions of the customer in order to initiate the product delivery. In this manner, the details of the implementation

of the order processor are hidden from the customer, making the experience similar without regard to the peculiarities of the implementations of particular vendors.

The vendor's order processor then initiates the delivery of the digital product to the customer. Upon completion of this delivery, the vendor system notifies the merchant of the successful fulfillment of the delivery request and the vendor records the fulfillment, preventing future access to that item in the customer's order.

For purposes of summarizing the invention, certain aspects, advantages and novel features of the invention have been described herein above. It is to be understood, however, that not necessarily all such advantages may be achieved in accordance with any particular embodiment of the invention. Thus, the invention may be embodied or carried out in a manner that achieves or optimizes one advantage or group of advantages as taught herein without necessarily achieving other advantages as may be taught or suggested herein.

Brief Description of the Drawings

These and other features will now be described with reference to the drawings summarized below. These drawings and the associated description are provided to illustrate embodiments of the invention, and not to limit the scope of the invention.

Figure 1 illustrates the principle components of a preferred embodiment of a system for anonymous delivery of digital goods.

Figure 2 illustrates a data flow diagram showing the transfer of information between a customer, an on-line merchant, and an on-line vendor in the preferred embodiment of the system.

Figure 3 illustrates a data flow diagram showing the transfer of information between a customer, an on-line merchant, and an on-line vendor in a first alternate embodiment of the system.

Figure 4 illustrates a data flow diagram showing the transfer of information between a customer, an on-line merchant, and an on-line vendor in a second alternate embodiment of the system.

Figure 5 is a sequence diagram showing, generally, the preferred embodiment of the system.

Figure 6 is a sequence diagram showing, generally, the first alternative embodiment of the system.

Figure 7 is a sequence diagram showing, generally, the second alternative embodiment of the system.

Figures 8A-B are a sequence diagram illustrating, in more detail, a process by which the system allows the delivery, by an on-line vendor, of digital products, purchased from a merchant, to a customer, in accordance with the first specific embodiment of the system.

Figure 9 illustrates an email message sent from the merchant to the customer in accordance with the preferred embodiment of the invention.

Figure 10 illustrates a Digital Product Receipt web page in accordance with the preferred embodiment of the invention.

Detailed Description of the Preferred Embodiment

In the following description, reference is made to the accompanying drawings, which show, by way of illustration, specific embodiments in which the invent may be practiced. Numerous specific details of these embodiments are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one skilled in the art that the present invention may be practiced without the specific details or with certain alternative components and methods to those described herein. In other instances, well-known methods, procedures, and components have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

Except where explicitly or implicitly indicated otherwise, the terms "merchant" and "vendor" refer to computer systems operated or controlled by a merchant or a vendor, respectively. Thus, process steps described as being performed by the "merchant" or the "vendor" are preferably automated steps performed by their respective computer systems. These steps are preferably implemented within software modules (programs) executed by one or more general purpose computers. Specially designed hardware could alternatively be used to perform certain operations. Process steps described as being performed by a "customer" are typically performed by a human

operator via an appropriate computing device, but could, alternatively, be performed by an automated agent.

Figure 1 illustrates the principal components of the preferred embodiment of a digital product delivery system 100, while Figure 2 illustrates the data flow in the digital product delivery system. A customer 102 can be any entity or individual that wishes to purchase goods or services from an on-line merchant 104. The merchant 104 is preferably an entity that sells products or services from a merchant web site 106, which is implemented using one or more physical servers 108. The customer 102 preferably uses a web browser 110 running on a computer 112. The computer is connected to the merchant server through a communications network 114, preferably the Internet.

In order to make purchases, the customer 102 typically browses through product information 202 concerning products available for purchase from the on-line merchant 104. After selecting a product or products that the customer 102 wishes to purchase a product order 204 is sent to the merchant 104. The product order 204 is preferably placed via a communication from the web browser 110 to the web site 106 operating on a server 108 maintained by the merchant 104. The customer 102 typically provides to the merchant 104 the customer's personal information, which includes identifying information and purchase information such as name, address phone number, and credit card information.

After the product order 204 is placed, the merchant 104 provides an order receipt 206 to the customer 102. The customer 102 then uses the order receipt 206 to issue a delivery request 208, preferably to the merchant 104 (i.e., the merchant's computer system 108). In some embodiments, the delivery request is alternatively transmitted to the vendor 116. This delivery request 208 trigger product delivery 210.

The ordered product is not provided by the merchant 104, but, preferably, by a third party vendor 116. The product delivery 210 is made to the customer via the communications network 114 from the vendor 116, and is performed in response to a fulfillment request 212 sent from the merchant 104 to an order processor 118. Preferably following, but in some embodiments concurrent to, the product delivery 210, the vendor 116 provides a delivery acknowledgement 214 to the merchant 104.

The flow of data in an alternative embodiment of the system is shown in Figure 3. In this embodiment, the information in the order receipt 206 allows the customer 102 to issue the delivery request 208 for the product delivery 210 to the vendor 116, rather than to the merchant 104 as in the preferred embodiment. In response to this delivery request 208, the vendor 116 issues a delivery notification 302 to the merchant 104. In response, if the delivery request 208 is valid, the merchant 104 sends a delivery approval 304 to the vendor 116 resulting in product delivery 210 from the vendor 116 to the customer/customer computer.

The flow of data in a second alternative embodiment is shown in Figure 4. In this embodiment, all data flow is as in the preferred embodiment, except for the product delivery 402, 404. In this embodiment, the product delivery from the vendor 116 to the customer 102 is performed in two legs or stages, via the merchant 104. Initially, the vendor 116 directs the first leg of the delivery 402 of the product to the merchant 104, and the merchant 104 then re-directs the second leg of the delivery 404 to the customer 102. As will be apparent to one skilled in the art, aspects of this embodiment may be combined with aspects of the first alternative embodiment to produce additional alternative embodiments.

Figure 5 illustrates the general process associated with the preferred embodiment of the invention depicted in Figure 2. The merchant displays product information 202 to the customer 102. The customer 102 places a product order 204 with the merchant 104. In response to the product order 204, the merchant 104 creates an order receipt 502 corresponding to the product order 204. The merchant 104 also generates an order URL (Uniform Resource Locator) 504 which contains information, securely encrypted and encoded, identifying the particular product order 204 which caused its creation. This order URL is then sent to the customer 102, preferably as part of a hyperlink within an order receipt 206.

At some later time, the customer 102 generates a request for the order URL that is part of the order receipt 206, such as by selecting the hyperlink. This URL request message represents the illustrated delivery request 208. The merchant then processes the order URL 506 in order to determine the product order 204 to which it corresponds. This is performed by decoding and decrypting a portion of the URL to determine the

order receipt ID. The merchant then verifies the validity of the order 508. This validity check confirms that the order is valid and that it has not yet been fulfilled. If the delivery request 208 is valid, then a fulfillment request 212 is issued to the vendor 116.

The fulfillment request 212 preferably includes only the information that is necessary to allow the vendor 116 to complete product delivery 210. This information may include the delivery address, e.g., the IP (Internet Protocol) address of the customer, as well as the product ID. The fulfillment request does not provide any of the customer's personal information such as customer name, email address, residence address, etc. In addition, the fulfillment request does not include other transaction information about the purchase such as method of payment or other identities of products purchased. Thus customer's privacy is therefore preserved.

The vendor 116 processes 510 the fulfillment request 212 and fulfills the order by effecting product delivery 210. After successful product delivery 210 to the customer's computer, the vendor issues a delivery acknowledgement 214 to the merchant 104, and the merchant marks the order as fulfilled 512. Once the order has been marked as fulfilled, the vendor may inhibit, or limit a number of, future downloads of the product by the consumer.

Figure 6 illustrates the general process corresponding to a first alternative embodiment, depicted in Figure 3. In this embodiment, the delivery request 208 from the customer 102 goes directly to the vendor 116, and the vendor 116 processes the order URL 602. This order URL contains sufficient information, such as the receipt ID and product information, that the vendor 116 can determine what product is desired and provide a meaningful delivery notification 302 to the merchant 104. The delivery notification 304 contains enough information, e.g. the receipt ID and an ID of the product desired, so that the merchant 104 can verify the order validity 508. Preferably, the merchant will determine at least whether the particular product has been paid for, and whether (or how many times) the product has been delivered to the customer. If the merchant 104 determines that the product has been purchased and not previously delivered (or delivered less than a threshold number of times), then the merchant 104 will issue a delivery approval 304 to the vendor 116. It is possible, in alternate embodiments, for the initial delivery notification 302 to contain only the receipt ID and

for all additional information needed to deliver the correct product to the customer 102 to come from the merchant 104 in the delivery approval 304. Upon receiving the delivery approval 304, the vendor 116 will process the order 510 and make the product delivery 210. Upon completion of the product delivery 210, the vendor 116 issues a delivery acknowledgement 214 to the merchant 104 and the order is marked as fulfilled 512. In this embodiment of the invention the vendor 116 to configures its order processor 118 so that it behaves in the same manner as the merchant's server 108 behaved in the preferred embodiment. The order processor 118 of the vendor 116 is also configured to interface with software on the merchant server 108 that handles validation and verification of the order.

Figure 7 illustrates the general process involved in the second alternative embodiment of the invention, depicted in Figure 4. The steps of this process are substantially the same as in the preferred embodiment except for those dealing delivery of the product from the vendor to the customer 402, 404. Rather than directly delivering the product to the customer in a single delivery leg, as in the preferred embodiment, the delivery is effected with two delivery legs. The vendor 116 initially directs the delivery of the product to the merchant 104 in a first delivery leg 701, and the merchant redirects the delivery to the customer in a second delivery leg 702. The redirection of delivery may be performed by forwarding by the merchant 104 of the delivery received from the vendor 116 to the customer 102. The first leg of the product delivery 402 contains sufficient information for the merchant 104 to reroute the delivery 702. This information may include complete final destination information, but is more likely to simply include an identifier that designates the order receipt to which this product delivery 402 corresponds. In this manner, all information about the customer 102, including the delivery address of the customer 102 may be hidden from the vendor 116.

Figures 8A-B illustrate a more detailed sequence flow of the preferred embodiment of the invention (previously illustrated in Figures 1, 2, and 5) involving the activities of a purchase handler 802, rights manager 804, and database 806 operated by the merchant 104. The merchant purchase handler 802 provides the product information 202 to the customer 102 and receives the product order 204 from the customer 102. The

purchase handler then initiates the creation of a receipt 808 by the rights manager 804. The rights manager creates a receipt database entry 810, which preferably contains all the information that may be used at a later date for processing or tracking the purchase. This may include the customer 102 name, address, and purchase information, as well as the details of the order including product ordered, quantity, price, and other characteristics. The rights manager 804 then Triple DES encrypts the receipt ID 812 and BASE64 encodes it 814. Other encryption and encoding schemes may be substituted for Triple DES and Base64. The rights manager 804 creates a receipt URL 816 based on the encrypted and encoded receipt ID. This URL is then included in a mail message, such as shown in Figure 9, and sent to the customer 102 as the order receipt 206. The order receipt 206 may alternatively be in the form of a web page. In the example shown in Figure 9, the string following the last forward slash of the URL is the encrypted and encoded receipt ID.

When the customer 102 decides to initiate delivery of the products ordered he or she can provide a receipt response 818, by accessing the receipt URL that was sent in the order receipt. This is preferably done using a web browser 110 operating on the customer's 102 computer 112. As shown in Figure 8A, when the customer 102 accesses this URL the rights manager 804 decodes the receipt ID 820, and decrypts the receipt ID 822 based on the secret key used to previously encrypt the receipt ID 812. The rights manager 804 requests the order information 824 from the database 806 and prepares a receipt page 828 based on the order information 826 returned from the database 806. This receipt page is preferably an HTML document which contains a list of the products ordered and other information relating to the product order including the number of products ordered. For each listed product, the receipt page also includes an HTML link that can be selected to access the product. An example of such a receipt page is shown in Figure 10. The receipt page is presented 830 to the customer 102.

The customer may issue a delivery request 208 for one or more products by clicking on the link on the receipt page. The rights manager 804 will then gather customer access information 832. This may include the IP address from which the customer is requesting delivery, as well as the browser ID, and other access related

information. The rights manager 804 will then update the access information in the database 806.

The rights manager 804 will then instigate the handling of the fulfillment of the delivery request 836. The detailed interaction between the rights manager 804 and the vendor 116 will vary based upon the manner in which the vendor's order processor 118 is configured. The fulfillment request 212 may be a simple redirect of the HTTP request from the customer to the vendor, or may be a series of requests and actions that simulate the access of an interactive user. In this manner it is possible for the product delivery system to provide the same user interface and experience to the customer 102, for different instantiations of the vendor side order processor 118. This is done in the preferred embodiment by the creation of different fulfillment handlers 836 corresponding to the different vendors 116 that work with the merchant 104. In some instantiations of the fulfillment handler 836, the fulfillment handler will authenticate the customer 102 as a valid customer and transfer the customer 102 to the vendor's order processor 118. For other vendors, the invoked fulfillment handler 836 initiates the product delivery 210 to the customer 102. The vendor's order processor 118 is given a secure hash of information, including the product to be delivered, and the customer address for delivery, as well as other information. This then allows the vendor 116 to complete the product delivery. The actions of the fulfillment handler 836 may cause the vendor 116 to directly deliver the product to the customer 102 for some types of product interfaces and to send the product to the merchant 104 for redirection or forwarding to the customer 102. The choice of which to do is done preferably, to maintain as simple and uniform an interface and shopping experience for the customer 102. In this manner a single embodiment of the delivery system may exhibit data flows as in Figures 2 and 4.

Upon completion of product delivery, 210 the rights manager 804 relies on positive feedback of delivery acknowledgement 214 from the vendor 116. Based upon this feedback, the rights manager 804 updates the fulfillment information 838 in the database 806. The rights manager 804 has information about attempted fulfillment from the invocation of the fulfillment handler and relies on information from the vendor 116 on completed product delivery 210. The onus is on the vendor to ensure that the

delivery acknowledgment 214 is sent to the merchant 104, lest the vendor 116 be left open to the possibility of being vulnerable to excessive fulfillment requests. Business practice determines the number, if any, of fulfillment requests beyond those purchased that will be allowed.

Although the invention has been described in terms of certain preferred embodiments, other embodiments that are apparent to those of ordinary skill in the art, including embodiments which do not provide all of the features and advantages set forth herein, are also within the scope of this invention. Accordingly, the scope of the invention is defined by the claims that follow. In the method claims, reference characters are used for convenience of description only, and do not indicate a particular order for performing the method.